Redes

Daniel Barrantes Esquivel

Autrum Transfer Protocol (ATP), es un protocolo creado durante los años 90 para el envío de mensaje (este utilizaba el puerto TCP/666), este se volvió muy popular entre las personas jóvenes de la época que tenían acceso a una red, este protocolo era capaz de transportar cualquier carácter visible ASCII, parte de lo emocionante de este protocolo era lograr enviar los mensajes de forma cifrada y el proceso era enteramente manual, lo cual quiere decir que las personas involucradas en la transmisión conocían las llaves para cifrar y descifrar mensajes. ATP se ha puesto de moda en el 2022, el problema es que ATP es un protocolo sumamente débil en términos de seguridad y además usa un puerto poco convencional como lo es TCP/666, con el fin de evaluar sí es posible implementar una versión segura de este protocolo, se le solicita responder las siguientes preguntas:

a. ¿Es posible enviar datos que no sean HTTPs sobre el puerto 443? Justifique su respuesta. (10 pts)

El puerto 443 es el puerto universal para todo trafico cifrado en internet, por lo que para poder enviar datos sobre el puerto 443 diferente a HTTPS este debe ser capaz de transferir datos de una manera segura, para esto debe instalar un certificado SSL en su servidor, SSL encriptará todos los datos transferidos hasta su finalización. Para que tus datos no sean fácilmente leídos o incluso robados por otros, y asi poder transferir los datos de forma segura a traves del puerto 443.

b. Suponiendo que creamos el protocolo ATP over SSL (ATPs), describa un subprotocolo para el establecimiento de una conexión SSL. (40 pts)

Cuando una web está protegida mediante SSL, las conexiones entre un cliente y el servidor se cifran. y asi haciendo una conexión más segura. Suponiendo que creamos el protocolo ATPs podriamos tener un sub-protocolo que nos indique la completitud del paquete entre el cliente y servidor, si el paquete está incompleto este no establece una conexión SSL, sino que genera un mensaje de alerta indicando que algo anda mal con el paquete, en caso de que el paquete llegue completo, este establece la conexión SSL y genera mensajes indicando que está activo, en caso de no estarlo o tener algun fallo analizando el paquete tambien lo indica, por lo que sería un protocolo de verificacion de paquetes y del estado del mismo hasta que la conexion con SSL se cierre.

c. Si existe el protocolo ATPs, ¿Es posible transportar ATPs sobre HTTPs? Justifique su respuesta. (10 pts)

Si existe el protocolo ATPs siendo la s "Secure" (Es decir, ATP sobre SSL) y sabiendo que este protocolo es para el envio de mensajes (Caracteres visibles ASCII). Sí, sería posible transportar ATPs sobre HTTPs, dado que este ultimo protocolo se usa para la transferencia de datos seguros por lo que al transportar ATPs sobre este lo que haria es que el dato de ATPs lo envia o transfiere mediante el protocolo HTTPs.

d. Desde un punto de vista de firewalls, ¿Porqué sería muy conveniente usar el puerto TCP/80 en lugar de puerto TCP/666?.

Sería conveniente por el hecho de que el puerto TCP/80 es uno de los muchos "Well-Known Port" existentes a diferencia del puerto TCP/666 que es un puerto no convencional por lo que desde un punto de vista de firewalls no es muy recomendado por lo que es mucho mejor usar el puerto TCP/80 dado que es más sencillo de detectar y usar, entre otras cosas.

2. Explique detalladamente el funcionamiento de RSA. (30 pts)

Este método se basa en ciertos principios de la teoría de los números.

1. Seleccionar dos números primos grandes, p y q (generalmente de 1024 bits).
2. Calcular n = p X q y z = (p - 1) X (q - 1).
3. Seleccionar un número primo con respecto a z, llamándolo d.
4. Encontrar e tal que e X d = 1 mod z

Al calcular esos parametro el algoritmo puede iniciar, para esto dividimos el texto llano (considerado como una cadena de bits) en bloques, para que cada mensaje de texto llano, P, caiga en el intervalo $0 \leq P < n$. Esto puede hacerse agrupando el texto llano en bloques de k bits, donde k es el entero más grande para el que 2 elevado a la "k" < n es verdad.

Para encriptar un mensaje, P, calculamos C = P elevado a la "e" (mod n). Para desencriptar C, calculamos P = C elevado a la "d" (mod n). Puede demostrarse que, para todos los P del intervalo especificado, las funciones de encriptación y desencriptación son inversas. Para ejecutar la encriptación, se necesitan e y n. Para llevar a cabo la desencriptación, se requieren d y n. Por tanto, la clave pública consiste en el par (e, n), y la clave privada consiste en (d, n).